

## COPYWRITE PROTECTION SYSTEM

**Publication number:** JP10003746

**Publication date:** 1998-01-06

**Inventor:** SAKAI YASUYUKI; YAMAGISHI ATSUHIRO; TAKEDA EISAKU

**Applicant:** MITSUBISHI ELECTRIC CORP

**Classification:**

**- International:** G11B20/10; G09C1/00; H04L9/08; G11B20/10; G09C1/00; H04L9/08; (IPC1-7): G11B20/10; G09C1/00; H04L9/08

**- European:** G11B20/00P

**Application number:** JP19960151117 19960612

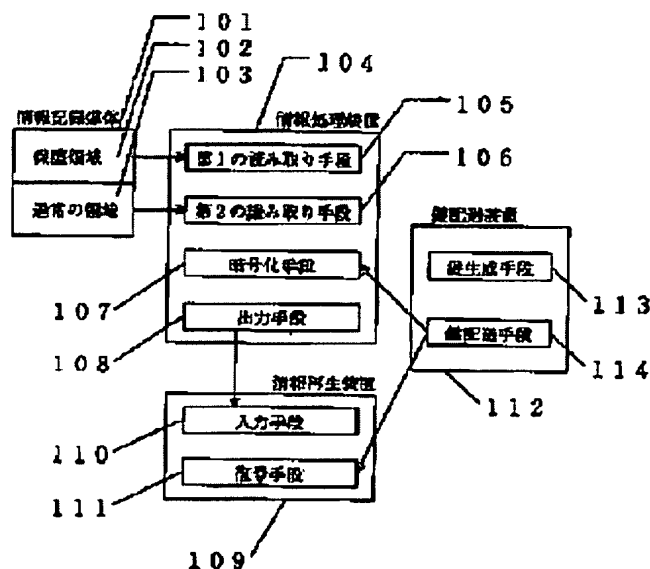
**Priority number(s):** JP19960151117 19960612

Report a data error here

### Abstract of JP10003746

**PROBLEM TO BE SOLVED:** To prevent the illicit duplication of digital information and to protect the right of a writer by recording enciphered digital information on an information recording medium and providing this medium with the following elements.

**SOLUTION:** The information recording medium 101 is provided with a protection region 102 where first encryption key is recorded and an ordinary region 103 where the enciphered digital information is recorded by using this first encryption key. An information processor 104 has a first reading means 105 for reading the first encryption key, a second reading means 106 for reading the digital information and an enciphering means 107 for enciphering the first encryption key with second encryption key. An information reproducing device 109 has an input means 110 to be inputted with the first encryption key and digital information outputted from an output means 108 and a decoding means 111 for decoding the enciphered first encryption key and digital information. A key distributing device 112 has a key forming means 113 for forming the second encryption key and a key distributing means 114 for distributing the formed second encryption key to the information processor 104 and the information reproducing device 109.



Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-3746

(43) 公開日 平成10年(1998) 1月6日

(51) Int.Cl. <sup>9</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 1 1 B 20/10		7736-5D	G 1 1 B 20/10	H
G 0 9 C 1/00	6 3 0	7259-5 J	G 0 9 C 1/00	6 3 0 D
H 0 4 L 9/08			H 0 4 L 9/00	6 0 1 D

審査請求 未請求 請求項の数 2 O L (全 4 頁)

(21) 出願番号 特願平8-151117

(22) 出願日 平成8年(1996) 6月12日

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 酒井 康行

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(72) 発明者 山岸 篤弘

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(72) 発明者 竹田 榮作

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

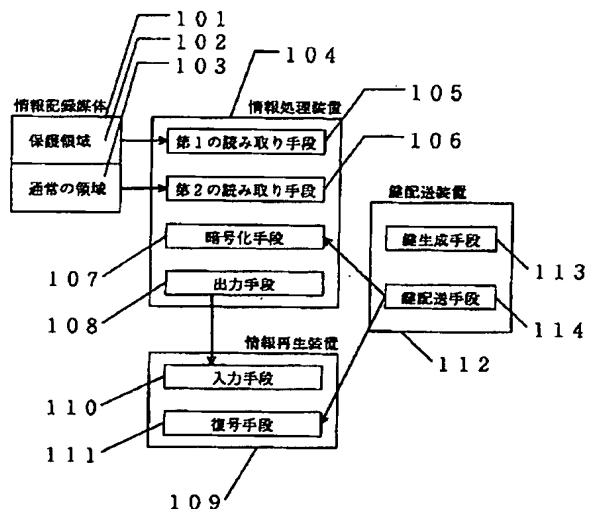
(74) 代理人 弁理士 宮田 金雄 (外3名)

(54) 【発明の名称】 著作権保護システム

(57) 【要約】

【課題】 著作者の権利を保護できる著作権保護システムを得ること。

【解決手段】 (a) 第1の暗号化鍵が記録される保護領域102と、第1の暗号化鍵を用いて暗号化されたデジタル情報が記録された通常の領域103とを備えた情報記録媒体101; (b) 第1の暗号化鍵を読み取る読み取り手段105と、デジタル情報を読み取る読み取り手段106と、第1の暗号化鍵を第2の暗号化鍵で暗号化する暗号化手段107とを備えた情報処理装置104; (c) 暗号化された第1の暗号化鍵と、暗号化されたデジタル情報とを復号する復号手段111を備えた情報再生装置109; (d) 第2の暗号化鍵を生成する鍵生成手段113と、生成された第2の暗号化鍵を情報処理装置104と情報再生装置109とに配送する鍵配送手段114とを備えた鍵配送装置112; とで構成する。



## 【特許請求の範囲】

【請求項1】 以下の要素を備えた著作権保護システム。

(a) 情報の読み出しに特別な手段を必要とする保護領域と、情報の読み出しに特別な手段を必要としない通常の領域とを設け、前記保護領域には第1の暗号化鍵が記録され、前記通常の領域には前記第1の暗号化鍵を用いて暗号化されたデジタル情報が記録された情報記録媒体；

(b) 前記第1の暗号化鍵を読み取る第1の読み取り手段と、前記デジタル情報を読み取る第2の読み取り手段と、前記第1の暗号化鍵を第2の暗号化鍵で暗号化する暗号化手段と、前記暗号化された第1の暗号化鍵と前記暗号化されたデジタル情報を出力する出力手段とを備えた情報処理装置；

(c) 前記出力手段より出力された、前記暗号化された第1の暗号化鍵と前記暗号化されたデジタル情報が入力される入力手段と、前記暗号化された第1の暗号化鍵と、前記暗号化されたデジタル情報とを復号する復号手段を備えた情報再生装置；

(d) 前記第2の暗号化鍵を生成する鍵生成手段と、生成された前記第2の暗号化鍵を前記情報処理装置と前記情報再生装置とに配送する鍵配送手段とを備えた鍵配送装置。

【請求項2】 前記鍵配送装置の前記鍵生成手段は、前記鍵配送装置のID情報と、前記情報処理装置のID情報と、前記情報再生装置のID情報とに基づいて暗号化鍵を生成することを特徴とする請求項1記載の著作権保護システム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、デジタル情報の不正な複製を防ぎ、著作権者の権利を保護できる著作権保護システムに関する。

## 【0002】

【従来の技術】従来のDVD(Digital Video Disc)を再生する装置について説明する。

【0003】図2は、DVDを再生するための従来の光ディスクシステムである。図において201はDVD再生装置、202はディスク、203はCD-ROMデコーダ、204は復調回路、205は誤り訂正回路、206はマルチプレクサ、207はバスインタフェースである。DVD再生装置201はDVDとCD-ROMの両方のディスクを再生できるように構成されている。次に動作を説明する。ディスク202から読み出されたデジタル情報は、CD-ROMデコーダ203および復調回路204に入力される。CD-ROMデコーダ203ではCD-ROMの場合の復調、誤り訂正が行われる。復調回路204ではディスクから読み出された信号をデジタル情報に復調する。復調されたデジタル情報は、誤り訂正回路205に入力され、DVDフォーマットの情報の誤り訂正を行う。マルチプレクサ206では、ディスク202がDVD、CD-ROMのいずれであるかに応じて情報を選択し、バスインタフェース207に出力する。

## 【0004】

【発明が解決しようとする課題】従来のDVDを再生する光ディスクシステムは、ディスクに記録されているデジタル情報は暗号化されておらず、また、再生する際にも暗号化は施されず、記録されている情報をそのまま再生していた。そのため、ディスクに記録されているデジタル情報の複製を作ることが容易であり、情報の著作権者の権利を保護することが困難であるという課題があった。

【0005】本発明の目的は、係る課題を解決するためになされたもので、デジタル情報の複製を作ることが困難で、著作権者の権利を保護することができる著作権保護システムを得ることにある。

## 【0006】

【課題を解決するための手段】本発明の請求項1に係る著作権保護システムは、以下の要素を備えたものである。

(a) 情報の読み出しに特別な手段を必要とする保護領域と、情報の読み出しに特別な手段を必要としない通常の領域とを設け、前記保護領域には第1の暗号化鍵が記録され、前記通常の領域には前記第1の暗号化鍵を用いて暗号化されたデジタル情報が記録された情報記録媒体；

(b) 前記第1の暗号化鍵を読み取る第1の読み取り手段と、前記デジタル情報を読み取る第2の読み取り手段と、前記第1の暗号化鍵を第2の暗号化鍵で暗号化する暗号化手段と、前記暗号化された第1の暗号化鍵と前記暗号化されたデジタル情報を出力する出力手段とを備えた情報処理装置；

(c) 前記出力手段より出力された、前記暗号化された第1の暗号化鍵と前記暗号化されたデジタル情報が入力される入力手段と、前記暗号化された第1の暗号化鍵と、前記暗号化されたデジタル情報とを復号する復号手段を備えた情報再生装置；

(d) 前記第2の暗号化鍵を生成する鍵生成手段と、生成された前記第2の暗号化鍵を前記情報処理装置と前記情報再生装置とに配送する鍵配送手段とを備えた鍵配送装置。

【0007】本発明の請求項2に係る著作権保護システムは、前記鍵配送装置の前記鍵生成手段は、前記鍵配送装置のID情報と、前記情報処理装置のID情報と、前記情報再生装置のID情報とに基づいて暗号化鍵を生成するものである。

## 【0008】

## 【発明の実施の形態】

実施の形態1. 本発明による著作権保護システムの一実施の形態を、図1に基づいて説明する。図1は、本実施の形態による著作権保護システムの構成図である。図において、101は情報記録媒体、102は保護領域、103は通常の領域、104は情報処理装置、105は第1の読み取り手段、106は第2の読み取り手段、107は暗号化手段、108は出力手段、109は情報再生装置、110は入力手段、111は復号手段、112は鍵配送装置、113は鍵生成手段、114は鍵配送手段である。

【0009】次に動作を説明する。情報記録媒体101は、例えば、DVDやCD-ROMなどの光ディスクで、情報処理装置104は、例えば、光ディスクを読み取るドライブで、情報再生装置109は、例えば、パーソナルコンピュータで、鍵配送装置112は、例えば、PCカードやICカードである。まず、情報記録媒体101の記録領域について説明する。情報記録媒体101は、デジタル情報を記録する領域を2種類に分ける。一方の領域は、読み取りに特別な手段を必要とする保護領域102で、他の一方の領域は、読み取りに特別な手段を必要としない通常の領域103である。保護領域102に記録された情報は、情報再生装置109、例えばパーソナルコンピュータ上のデバイスドライバ等では読み取ることができず、情報処理装置104の第1の読み取り手段105のみによって情報が読み出され、読み出された情報は、情報処理装置104の外に直接出力することはできない。通常の領域103に記録された情報は、第2の読み取り手段106及び出力手段108を介して、情報処理装置104の外部に出力することができる。通常の領域103には、暗号化されたデジタル情報が記録される。保護領域102には、通常の領域103に記録する情報を暗号化する際に用いた第1の暗号化鍵が記録される。次に、情報処理装置104から情報再生装置109へデジタル情報を送信する手順を説明する。まず、鍵配送装置112内の鍵生成手段113において、第2の暗号化鍵を生成する。生成された第2の暗号化鍵は、鍵配送手段114により情報処理装置104内の暗号化手段107、及び情報再生装置109内の復号手段111に配送される。次に、情報処理装置104内では、まず、第1の読み取り手段105により読み出された保護領域102に記録されている第1の暗号化鍵を、暗号化手段107により、第2の暗号化鍵を用いて暗号化する。暗号化された第1の暗号化鍵と、第2の読み取り手段106により読み出された暗号化されたデジタル情報を、出力手段108を介して情報再生装置109に出力する。次に、情報再生装置109内ではまず、入力手段110を介して、暗号化された第1の暗号

化鍵及び暗号化されたデジタル情報を受信する。次に、復号手段111において、暗号化された第1の暗号化鍵を、第2の暗号化鍵を用いて復号する。次に、暗号化されたデジタル情報を、第1の暗号化鍵を用いて復号する。以上の動作で、情報記録媒体101内の通常の領域103に記録されているデジタル情報は、情報再生装置109で再生される。本実施の形態の著作権保護システムは、情報記録媒体に記録されたデジタル情報は暗号化されているので、デジタル情報の不正な複製を防ぐことができ、著作権者の権利を保護することができる。

【0010】実施の形態2. 前記実施の形態1では、鍵生成手段113において単独に第2の暗号化鍵を生成していたが、情報処理装置104、情報再生装置109及び鍵配送装置112にそれぞれのID情報を設け、それらのID情報に基づいて第2の暗号化鍵を生成してもよい。

【0011】実施の形態3. 前記実施の形態1では、暗号化手段107及び復号手段109に、鍵配送手段114より同じ暗号化鍵を配送していたが、公開鍵暗号方式を用いることもできる。

【0012】実施の形態4. 前記実施の形態1では、情報再生装置109を例えばパーソナルコンピュータとしていたが、DVDプレーヤーなどのオーディオ機器など、デジタル情報を再生する装置なら何でもよい。また、鍵配送装置112には、オーディオ機器のリモコン装置等を用いることもできる。

【0013】実施の形態5. 前記実施の形態1では、情報記録媒体101は、例えば光ディスクとしていたが、デジタル情報を記録する媒体であればよい。

【0014】

【発明の効果】以上のように、本発明による著作権保護システムは、デジタル情報の不正な複製を防ぐことができ、著作権者の権利を保護することができる効果がある。

【図面の簡単な説明】

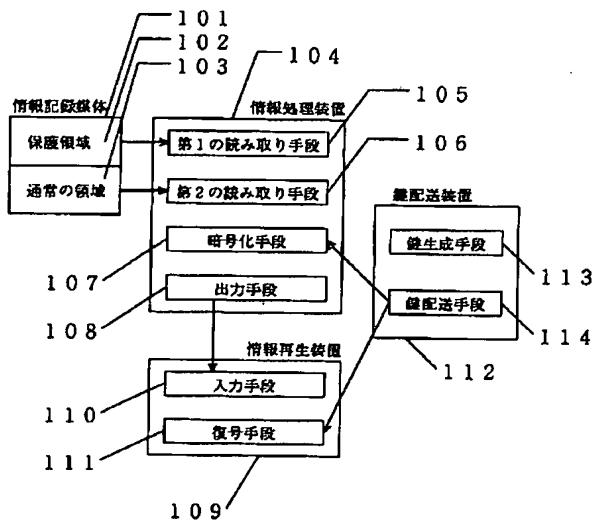
【図1】 本発明の著作権保護システムを説明する図である。

【図2】 従来の光ディスクシステムの構成図である。

【符号の説明】

101 情報記録媒体、102 保護領域、103 通常の領域、104 情報処理装置、105 第1の読み取り手段、106 第2の読み取り手段、107 暗号化手段、108 出力手段、109 情報再生装置、110 入力手段、111 復号手段、112 鍵配送装置、113 鍵生成手段、114 鍵配送手段。

【図1】



【図2】

